

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-マコード (参考)
H04B 1/707		G06F 7/58	B 5J104
G06F 7/58		G09C 1/00	B 5K022
G09C 1/00	650	H04J 13/00	D
H04L 9/26		H04L 9/00	659

審査請求 有 請求項の数32 O L (全21頁)

(21)出願番号	特願2001 - 87480( P 2001 - 87480)	(71)出願人	396020800 科学技術振興事業団 埼玉県川口市本町 4 丁目 1 番 8 号
(22)出願日	平成13年 3 月26日(2001.3.26)	(71)出願人	597044841 梅野 健 東京都小金井市貫井北町 4 - 2 - 1 独立 行政法人通信総合研究所内
		(74)代理人	100095407 弁理士 木村 満 (外 1 名)

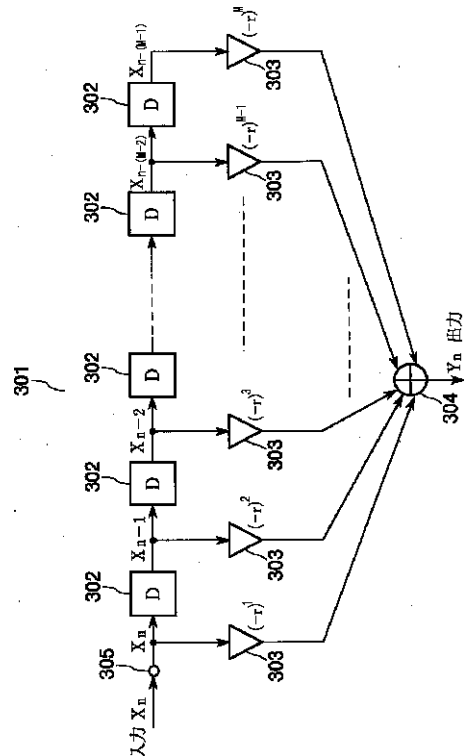
最終頁に続く

(54) 【発明の名称】 擬似乱数列の出力装置、送信装置、受信装置、通信システム、フィルタ装置、擬似乱数列の出力方法、送信方法、受信方法、フィルタ方法、プログラム、ならびに、情報記録媒体

(57) 【要約】

【課題】 擬似乱数列を生成するフィルタ装置等を提供する。

【解決手段】 所定の実インパルス定数 $r$  ( $-1 < r < 1$ )に対する F I R フィルタ 3 0 1 は、チップ長 $D$ の拡散符号系列の入力信号の入力を端子 3 0 5 で受け付け、入力信号を、それぞれ $0$ 、 $D$ 、 $2D$ 、 $3D$ 、...、 $(N-1)D$ だけ遅延させた複数の信号を遅延回路 3 0 2 により出力し、遅延されて出力された複数の信号のそれぞれを、当該遅延時間が $T$ である場合、増幅器 3 0 3 により $(-r)^{1 + T/D}$ 倍して出力し、増幅されて出力された複数の信号の総和、すなわち、最適カオス型拡散符号系列を、加算器 3 0 4 により出力する。



## 【特許請求の範囲】

【請求項 1】所定の実インパルス定数  $r$  ( $-1 < r < 1$ ) と、所定の実数定数  $C$  ( $C > 0$ ) と、に対して、長さ  $N$  ( $N \geq 1$ ) の擬似乱数列を出力する出力装置であって、系列初期値として長さ  $L$  ( $L \geq 1$ ) の拡散符号  $z[1], z[2], \dots, z[L]$  の入力を受け付ける系列受付部と、前記入力を受け付けた  $z[1], z[2], \dots, z[L]$  から、所定の整数  $M$  ( $1 \leq M \leq N, M+N < L$ ) に対して

## 【数 1】

$$\begin{aligned} z'[1] &= C \sum_{j=1}^M (-r)^{M+1-j} z[j], \\ z'[2] &= C \sum_{j=1}^M (-r)^{M+1-j} z[j+1], \\ &\vdots \\ z'[N] &= C \sum_{j=1}^M (-r)^{M+1-j} z[j+N-1] \end{aligned}$$

$$2 - \sqrt{3} - 0.1 \leq r \leq 2 - \sqrt{3} + 0.1$$

を満足することを特徴とする請求項 1 または 2 に記載の出力装置。

【請求項 4】伝送信号の入力を受け付ける信号受付部と、請求項 1 から 3 のいずれか 1 項に記載の長さ  $N$  の擬似乱数列を出力する出力装置と、前記入力を受け付けられた伝送信号を、前記出力された長さ  $N$  の擬似乱数列を拡散符号として、スペクトラム拡散する拡散部と、前記スペクトラム拡散された結果の信号を送信する信号送信部と、を備えることを特徴とする送信装置。

【請求項 5】拡散符号  $z[1], z[2], \dots, z[L]$  を選択する選択部と、前記選択された拡散符号  $z[1], z[2], \dots, z[L]$  を送信するパラメータ送信部と、をさらに備え、前記出力装置は、前記選択された拡散符号  $z[1], z[2], \dots, z[L]$  を系列初期値として受け付けることを特徴とする請求項 4 に記載の送信装置。

【請求項 6】拡散符号  $z[1], z[2], \dots, z[L]$  を受信するパラメータ受信部をさらに備え、前記出力装置は、前記受信された拡散符号  $z[1], z[2], \dots, z[L]$  を系列初期値として受け付けることを特徴とする請求項 4 に記載の送信装置。

【請求項 7】信号を受信する信号受信部と、請求項 1 から 3 のいずれか 1 項に記載の長さ  $N$  の擬似乱数列を出力する出力装置と、前記受信された信号を、前記出力された長さ  $N$  の擬似乱

を満す  $z'[1], z'[2], \dots, z'[N]$  を計算する計算部と、

前記  $z'[1], z'[2], \dots, z'[N]$  を擬似乱数列として出力する出力部と、

を備えることを特徴とする出力装置。

【請求項 2】前記長さ  $L$  の拡散符号は、 $M$  系列、ゴールド符号、嵩符号、ウォルシュ - アダムール直交符号、もしくは、チェビシェフ多項式により生成されるカオス符号であることを特徴とする請求項 1 に記載の出力装置。

10 【請求項 3】前記所定の実インパルス定数  $r$  は、【数 2】

数列を拡散符号として、スペクトラム逆拡散する逆拡散部と、

前記スペクトラム逆拡散された結果の信号を送信信号として出力する出力部と、

を備えることを特徴とする受信装置。

【請求項 8】拡散符号  $z[1], z[2], \dots, z[L]$  を選択する選択部と、

30 前記選択された拡散符号  $z[1], z[2], \dots, z[L]$  を送信するパラメータ送信部と、

をさらに備え、

前記出力装置は、前記選択された拡散符号  $z[1], z[2], \dots, z[L]$  を系列初期値として受け付けることを特徴とする請求項 7 に記載の受信装置。

【請求項 9】拡散符号  $z[1], z[2], \dots, z[L]$  を受信するパラメータ受信部をさらに備え、

40 前記出力装置は、前記受信された拡散符号  $z[1], z[2], \dots, z[L]$  を系列初期値として受け付けることを特徴とする請求項 7 に記載の受信装置。

【請求項 10】請求項 5 に記載の送信装置と、請求項 9 に記載の受信装置と、

を備え、

前記受信装置は、前記送信装置から送信された拡散符号  $z[1], z[2], \dots, z[L]$  を受信し、

前記受信装置は、前記送信装置から送信された信号を受信することを特徴とする通信システム。

【請求項 11】請求項 6 に記載の送信装置と、

請求項 8 に記載の受信装置と、

を備え、

50 前記送信装置は、前記受信装置から送信された拡散符号

$z[1], z[2], \dots, z[L]$ を受信し、  
前記受信装置は、前記送信装置から送信された信号を受信することを特徴とする通信システム。

【請求項 1 2】所定の実インパルス定数  $r$  ( $-1 < r < 1$ ) と、所定の実数定数  $C$  ( $C \neq 0$ ) と、に対するフィルタ装置であって、  
チップ長  $D$  の入力信号の入力を受け付ける入力端子と、前記入力を受け付けられた入力信号を、それぞれ  $0, D, 2D, 3D, \dots, (N-1)D$  だけ遅延させた複数の信号を出力する遅延部と、

$$2 - \sqrt{3} - 0.1 \leq r \leq 2 - \sqrt{3} + 0.1$$

を満足することを特徴とする請求項 1 2 に記載のフィルタ装置。

【請求項 1 4】前記フィルタ装置の遅延部、増幅部、および、加算部は、ASIC (Application Specific Integrated Circuit)、DSP (Digital Signal Processor)、もしくは、FPGA (Field Programmable Gate Array) によって構成されることを特徴とする請求項 1 2 または 1 3 に記載のフィルタ装置。

【請求項 1 5】所定の実インパルス定数  $r$  ( $-1 < r < 1$ ) と、所定の実数定数  $C$  ( $C \neq 0$ ) と、に対して、長さ  $N$  ( $N \geq 1$ ) の擬似乱数列を出力する出力方法であって、系列初期値として長さ  $L$  ( $L \geq 1$ ) の拡散符号  $z[1], z[2], \dots, z[L]$  の入力を受け付ける系列受付工程と、前記入力を受け付けた  $z[1], z[2], \dots, z[L]$  から、所定の整数  $M$  ( $1 \leq M \leq N, M+N < L$ ) に対して

【数 4】

$$\begin{aligned} z'[1] &= C \sum_{j=1}^M (-r)^{M+1-j} z[j], \\ z'[2] &= C \sum_{j=1}^M (-r)^{M+1-j} z[j+1], \\ &\vdots \\ z'[N] &= C \sum_{j=1}^M (-r)^{M+1-j} z[j+N-1] \end{aligned}$$

$$2 - \sqrt{3} - 0.1 \leq r \leq 2 - \sqrt{3} + 0.1$$

を満足することを特徴とする請求項 1 5 または 1 6 に記載の出力方法。

【請求項 1 8】伝送信号の入力を受け付ける信号受付工程と、  
請求項 1 5 から 1 7 のいずれか 1 項に記載の出力方法により長さ  $N$  の擬似乱数列を出力して生成する生成工程と、  
前記入力を受け付けられた伝送信号を、前記生成された長さ  $N$  の擬似乱数列を拡散符号として、スペクトラム拡散する拡散工程と、

前記遅延されて出力された複数の信号のそれぞれを、当該遅延時間が  $T$  である場合、 $C(-r)^{1+T/D}$  倍して出力する増幅部と、

前記増幅されて出力された複数の信号の総和を出力する加算部と、

前記加算されて出力された信号を出力する出力端子と、を備えることを特徴とするフィルタ装置。

【請求項 1 3】前記所定の実インパルス定数  $r$  は、

【数 3】

を満たす  $z'[1], z'[2], \dots, z'[N]$  を計算する計算工程と、

前記  $z'[1], z'[2], \dots, z'[N]$  を擬似乱数列として出力する出力工程と、

を備えることを特徴とする出力方法。

【請求項 1 6】前記長さ  $L$  の拡散符号は、M 系列、ゴールド符号、嵩符号、ウォルシュ - アダマール直交符号、もしくは、チェビシェフ多項式により生成されるカオス符号であることを特徴とする請求項 1 5 に記載の出力方法。

【請求項 1 7】前記所定の実インパルス定数  $r$  は、

【数 5】

前記スペクトラム拡散された結果の信号を送信する信号送信工程と、

を備えることを特徴とする送信方法。

【請求項 1 9】拡散符号  $z[1], z[2], \dots, z[L]$  を選択する選択工程と、

前記選択された拡散符号  $z[1], z[2], \dots, z[L]$  を送信するパラメータ送信工程と、

をさらに備え、

前記生成工程では、前記選択された拡散符号  $z[1], z$

20  $[2], \dots, z[L]$  を系列初期値として受け付けることを特

徴とする請求項 18 に記載の送信方法。

【請求項 20】拡散符号  $z[1], z[2], \dots, z[L]$  を受信するパラメータ受信工程をさらに備え、前記生成工程では、前記受信された拡散符号  $z[1], z[2], \dots, z[L]$  を系列初期値として受け付けることを特徴とする請求項 18 に記載の送信方法。

【請求項 21】信号を受信する信号受信工程と、請求項 15 から 17 のいずれか 1 項に記載の出力方法により長さ  $N$  の疑似乱数列を出力する生成工程と、前記受信された信号を、前記生成された長さ  $N$  の疑似乱数列を拡散符号として、スペクトラム逆拡散する逆拡散工程と、前記スペクトラム逆拡散された結果の信号を伝送信号として出力する出力工程と、を備えることを特徴とする受信方法。

【請求項 22】拡散符号  $z[1], z[2], \dots, z[L]$  を選択する選択工程と、前記選択された拡散符号  $z[1], z[2], \dots, z[L]$  を送信するパラメータ送信工程と、をさらに備え、前記生成工程では、前記選択された拡散符号  $z[1], z[2], \dots, z[L]$  を系列初期値として受け付けることを特

$$2 - \sqrt{3} - 0.1 \leq r \leq 2 - \sqrt{3} + 0.1$$

を満足することを特徴とする請求項 24 に記載のフィルタ方法。

【請求項 26】コンピュータを、請求項 1 から 3 のいずれか 1 項に記載の出力装置として機能させることを特徴とするプログラム。

【請求項 27】コンピュータを、請求項 12 または 13 に記載のフィルタ装置として機能させることを特徴とするプログラム。

【請求項 28】コンピュータに、請求項 15 から 17 のいずれか 1 項に記載の出力方法を実行させることを特徴とするプログラム。

【請求項 29】コンピュータに、請求項 24 または 25 に記載のフィルタ方法を実行させることを特徴とするプログラム。

【請求項 30】請求項 26 から 29 のいずれか 1 項に記載のプログラムを記録したことを特徴とするコンピュータ読取可能な情報記録媒体（コンパクトディスク、フロッピー（登録商標）ディスク、ハードディスク、光磁気ディスク、デジタルビデオディスク、磁気テープ、または、半導体メモリを含む。）。

【請求項 31】請求項 1 から 3 のいずれか 1 項に記載の出力装置により出力される疑似乱数列を記録したことを特徴とするコンピュータ読取可能な情報記録媒体（コンパクトディスク、フロッピーディスク、ハードディスク、光磁気ディスク、デジタルビデオディスク、磁気テープ、または、半導体メモリを含む。）。

徴とする請求項 21 に記載の受信方法。

【請求項 23】拡散符号  $z[1], z[2], \dots, z[L]$  を受信するパラメータ受信工程をさらに備え、前記生成工程では、前記受信された拡散符号  $z[1], z[2], \dots, z[L]$  を系列初期値として受け付けることを特徴とする請求項 21 に記載の受信方法。

【請求項 24】所定の実インパルス定数  $r$  ( $-1 < r < 1$ ) と、所定の実数定数  $C$  ( $C > 0$ ) と、に対するフィルタ方法であって、

- 10 チップ長  $D$  の入力信号の入力を受け付ける入力工程と、前記入力を受け付けられた入力信号を、それぞれ  $0, D, 2D, 3D, \dots, (N-1)D$  だけ遅延させた複数の信号を出力する遅延工程と、前記遅延されて出力された複数の信号のそれぞれを、当該遅延時間が  $T$  である場合、 $C(-r)^{1 + T/D}$  倍して出力する増幅工程と、前記増幅されて出力された複数の信号の総和を出力する加算工程と、前記加算されて出力された信号を出力する出力工程と、
- 20 を備えることを特徴とするフィルタ方法。

【請求項 25】前記所定の実インパルス定数  $r$  は、  
【数 6】

$$2 - \sqrt{3} - 0.1 \leq r \leq 2 - \sqrt{3} + 0.1$$

【請求項 32】請求項 15 から 17 のいずれか 1 項に記載の出力方法により出力される疑似乱数列を記録したことを特徴とするコンピュータ読取可能な情報記録媒体（コンパクトディスク、フロッピーディスク、ハードディスク、光磁気ディスク、デジタルビデオディスク、磁気テープ、または、半導体メモリを含む。）。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、疑似乱数列の出力装置、送信装置、受信装置、通信システム、フィルタ装置、疑似乱数列の出力方法、送信方法、受信方法、フィルタ方法、プログラム、ならびに、情報記録媒体に関する。

【0002】特に、衛星通信、固定通信、携帯電話や PHS (Personal Handyphone System) などの陸上移动通信や GPS (Global Positioning System) などの測距分野で用いることができるスペクトラム拡散通信の非同期 CDMA (Code Division Multiple Access; 符号分割多元接続) 方式の拡散符号として使用できる疑似乱数列を出力するのに好適な出力装置、出力方法と、これを用いた送信装置、受信装置、通信システム、フィルタ装置、送信方法、受信方法、フィルタ方法、これらを実現するためのプログラム、ならびに、当該プログラムを記録したコンピュータ読取可能な情報記録媒体に関する。

【0003】

- 50 【従来の技術】従来から、スペクトラム拡散通信、符号

分割多重通信を実現する拡散符号として、線形帰還シフトレジスタ (Linear Feedback Shift Register ; L F S R ) によって作られる、M 系列、嵩符号、ゴールド系列等が提案されている。これらの拡散符号系列には、以下の 2 つの特徴がある。

【 0 0 0 4 】第 1 に、同じ符号同士の相関 ( 自己相関 ) に一つのピークを持ち、異なる符号同士の相関 ( 相互相関 ) は 0 である。これは、白色雑音 ( white noise ) の性質に極めて類似している。

【 0 0 0 5 】第 2 に、符号集合に含まれる異なる 2 つの拡散符号を選択した場合、いずれを選択してもその相互相関が 0 に近くなるように符号集合を構成した場合、符号集合に含まれる符号の数が、符号長 N に対して O(N) しかない。このため、符号の種類が少ない。

【 0 0 0 6 】一方、古くから T D M A ( Time Division Multiple Access ; 時分割多元接続 ) や F D M A ( Frequency Division Multiple Access ; 周波数分割多元接続 ) も知られている。非同期 C D M A 通信システムは、これらと異なり、信号の同期を積極的にとらなくとも、用いられる符号の相関特性を利用して、復号ができるという特徴を有する。このため、秘話性、秘匿性、耐干渉・妨害性、などに優れる。

【 0 0 0 7 】現在非同期 C D M A 通信システムは、実用化が進められており、I M T - 2 0 0 0 ( International Mobile Telecommunication 2000 ) という次世代無線通信の I T U ( International Telecommunication Union ) 標準規格として採用が決まっている。

【 0 0 0 8 】近年の研究により、非同期 C D M A 通信システムでは、符号間干渉ノイズの分散  $\sigma^2$  が、システムの性能を決めることがわかっている。この分散  $\sigma^2$  は、ゴ

$$C(s) \approx Const. \times (-r)^s \quad (0 < r < 1)$$

【 0 0 1 4 】特に、実インパルス定数 r が [ 数 8 ] を満たす場合、[ 数 9 ] のような最適相関関数の形をとる。

$$2 - \sqrt{3} - 0.1 \leq r \leq 2 - \sqrt{3} + 0.1$$

【 0 0 1 6 】

【 数 9 】

$$\sigma_{optimal} = \sqrt{3}(K - 1)/6N$$

【 0 0 1 7 】これは、同一ビット誤り率での同時接続ユーザー数 K が、擬似白色雑音を拡散符号として用いた場合の非同期 C D M A 通信システムのユーザー数の理論限界より 1 5 パーセントも増えるということである。この点については、以下の文献に開示されている。G . Mazzi ni , R . Rovatti , and G . Setti 「 Interference Minimization by Auto-Correlation Shaping in Asynchronous DS-CDMA Systems: Chaos-Based Spreading is Nearly Optimal 」 ( Electron . Lett . ( 1999 ) vol.35 , pp.1054-1055 )

ルド符号や嵩符号などの擬似白色雑音を拡散符号として用いる場合に、同時接続ユーザー数を K とし、符号長を N とすると、漸近的に  $\sigma^2 = (K-1)/3N$  であることが、たとえば以下の文献に開示されている。M . B . Pursley , 「 Performance Evaluation for Phased-Coded Spread-Spectrum Multiple-Access Communication-Part I: System Analysis 」 ( IEEE Trans . Communications , vol.25 ( 1977 ) pp.795-799. )

【 0 0 0 9 】ここで、「漸近的」とは、ユーザー数 K と、符号長 N とを大きくとった場合、という意味である。

【 0 0 1 0 】従来、非同期 C D M A 通信システムの性能の理論的限界は、この  $\sigma^2 = (K-1)/3N$  であると考えられていた。しかしながら、このような漸近的関係が成立するのは、拡散符号が、擬似白色雑音であるということに起因することもわかっていた。

【 0 0 1 1 】したがって、拡散符号が擬似白色雑音でない場合、すなわち、異なる符号の間にいくらかの相関がある場合には、性能の理論的限界が向上する可能性もあった。

【 0 0 1 2 】最近になって、拡散符号が擬似白色雑音である場合に比べて符号間干渉ノイズの分散  $\sigma^2$  が減少するような自己相関関数を持つ拡散符号の存在が発見された。すなわち、自己相関関数が符号のシフト量に対して、[ 数 7 ] のように指数関数的に減少する場合は、その干渉ノイズの分散  $\sigma^2$  は、擬似白色雑音の場合よりも小さくなる。

【 0 0 1 3 】

【 数 7 】

【 0 0 1 5 】

【 数 8 】

【 0 0 1 8 】また、同文献では、部分的傾きが極めて大きい多段線形写像を用いてカオスの拡散符号を構成することにより、[ 数 7 ] を満足する相関関数を近似的に模式できることが示されている。

【 0 0 1 9 】

【 発明が解決しようとする課題 】しかしながら、このような拡散系列を D S P ( Digital Signal Processor ) などを用いて実際に生成して携帯電話などで利用するためには、高速性と低消費電力が必要となるため、以下のような課題が発生していた。

【 0 0 2 0 】第 1 に、拡散符号が極めて大きな傾きの多段線形写像で構成されているため、D S P やコンピュータなどで計算を行うと、桁落ちが大きくなり、正確な結果が得られない、という問題があった。このため、物理

的な回路や装置を構成して、拡散符号を生成することは難しい、という課題があった。

【 0 0 2 1 】第 2 に、相関関数の減衰の様子を決定するパラメータを、任意の  $r$  ( $-1 < r < 1$ ) に対して自由自在に調整することができない、という課題があった。

【 0 0 2 2 】第 3 に、上記文献では、最適相関関数に近い相関関数を持つ多段線形写像の種類は少ないことが示されている。しかしながら、CDMA 通信システムを実現するためには、できるかぎり多種類の符号があった方がよい。このため、上記文献に開示される手法を用いるのでは、CDMA 通信システムを現実構成することは難しかった。

【 0 0 2 3 】第 4 に、線形シフトレジスタを用いて生成した拡散符号では、符号長  $N$  に対して、相関特性の良い符号の種類は、 $O(N)$  しかない。本来の符号の種類は、2 のべき乗に比例する数  $O(2^N)$  だけあるのに対して、これでは極めて少ない。このため、ユーザー数の増大に対応することが難しい。

【 0 0 2 4 】第 5 に、鍵空間が狭いため、解読に必要な手間が少ない。このため、通信セキュリティが弱くなってしまおうという問題が生ずる。

【 0 0 2 5 】これらの問題については、上記文献に開示される技術では、改善がなされていない。

【 0 0 2 6 】したがって、このような課題を解決しつつ、非同期 CDMA 通信システムに適した擬似乱数列 (PN (Pseudo Noise ; 擬似雑音) 系列ともいう。) からなる拡散符号の生成技術が強く望まれている。

【 0 0 2 7 】本発明は、非同期 CDMA 通信システムに適した擬似乱数列の出力装置、送信装置、受信装置、通信システム、フィルタ装置、擬似乱数列の出力方法、送信方法、受信方法、フィルタ方法、これらを実現するためのプログラム、ならびに、当該プログラムを記録したコンピュータ読取可能な情報記録媒体を提供することを目的とする。

【 0 0 2 8 】

【課題を解決するための手段】以上の目的を達成するため、本発明の原理にしたがって、下記の発明を開示する。

【 0 0 2 9 】本発明の第 1 の観点に係る出力装置は、所定の実インパルス定数  $r$  ( $-1 < r < 1$ ) と、所定の実数定数  $C$  ( $C > 0$ ) と、に対して、長さ  $N$  ( $N > 1$ ) の擬似乱数列を出力し、系列受付部と、計算部と、出力部と、を備え、以下のように構成する。

【 0 0 3 0 】すなわち、系列受付部は、系列初期値として長さ  $L$  ( $L > 1$ ) の拡散符号  $z[1], z[2], \dots, z[L]$  の入力を受け付ける。

【 0 0 3 1 】一方、計算部は、入力を受け付けた  $z[1], z[2], \dots, z[L]$  から、所定の整数  $M$  ( $1 \leq M \leq N, M+N < L$ ) に対して

【 0 0 3 2 】

【数 1 0】

$$z'[1] = C \sum_{j=1}^M (-r)^{M+1-j} z[j],$$

$$z'[2] = C \sum_{j=1}^M (-r)^{M+1-j} z[j+1],$$

⋮

$$z'[N] = C \sum_{j=1}^M (-r)^{M+1-j} z[j+N-1]$$

を満たす  $z'[1], z'[2], \dots, z'[N]$  を計算する。

【 0 0 3 3 】さらに、出力部は、 $z'[1], z'[2], \dots, z'[N]$  を擬似乱数列として出力する。

【 0 0 3 4 】また、本発明の出力装置において、長さ  $L$  の拡散符号は、 $M$  系列、ゴールド符号、嵩符号、ウォルシュ - アダムール直交符号、もしくは、チェビシェフ多項式により生成されるカオス符号であるように構成することができる。

【 0 0 3 5 】また、本発明の出力装置において、所定の実インパルス定数  $r$  は、【数 8】を満足するように構成することができる。

【 0 0 3 6 】本発明の第 2 の観点に係る送信装置は、信号受付部と、上記の出力装置と、拡散部と、信号送信部と、を備えるように構成する。

【 0 0 3 7 】ここで、信号受付部は、伝送信号の入力を受け付ける。

【 0 0 3 8 】一方、上記の出力装置は、長さ  $N$  の擬似乱数列を出力する。

【 0 0 3 9 】さらに、拡散部は、入力を受け付けられた伝送信号を、出力された長さ  $N$  の擬似乱数列を拡散符号として、スペクトラム拡散する。

【 0 0 4 0 】そして、信号送信部は、スペクトラム拡散された結果の信号を送信する。

【 0 0 4 1 】また、本発明の送信装置は、選択部と、パラメータ送信部をさらに備え、以下のように構成することができる。

【 0 0 4 2 】すなわち、選択部は、拡散符号  $z[1], z[2], \dots, z[L]$  を選択する。

【 0 0 4 3 】一方、パラメータ送信部は、選択された拡散符号  $z[1], z[2], \dots, z[L]$  を送信する。

【 0 0 4 4 】さらに、出力装置は、選択された拡散符号  $z[1], z[2], \dots, z[L]$  を系列初期値として受け付ける。

【 0 0 4 5 】また、本発明の送信装置は、パラメータ受信部をさらに備え、以下のように構成することができる。

【 0 0 4 6 】すなわち、パラメータ受信部は、拡散符号  $z[1], z[2], \dots, z[L]$  を受信する。

【 0 0 4 7 】一方、出力装置は、受信された拡散符号  $z[1], z[2], \dots, z[L]$  を系列初期値として受け付ける。

10

20

30

40

50

【0048】本発明の第3の観点に係る受信装置は、信号受信部と、上記の出力装置と、逆拡散部と、出力部と、を備え、以下のように構成する。

【0049】すなわち、信号受信部は、信号を受信する。

【0050】一方、出力装置は、長さNの擬似乱数列を出力する。

【0051】さらに、逆拡散部は、受信された信号を、出力された長さNの擬似乱数列を拡散符号として、スペクトラム逆拡散する。

【0052】そして、出力部は、スペクトラム逆拡散された結果の信号を伝送信号として出力する。

【0053】また、本発明の受信装置は、選択部と、パラメータ送信部をさらに備え、以下のように構成することができる。

【0054】すなわち、選択部は、拡散符号 $z[1]$ ,  $z[2]$ , ...,  $z[L]$ を選択する。

【0055】一方、パラメータ送信部は、選択された拡散符号 $z[1]$ ,  $z[2]$ , ...,  $z[L]$ を送信する。

【0056】さらに、出力装置は、選択された拡散符号 $z[1]$ ,  $z[2]$ , ...,  $z[L]$ を系列初期値として受け付ける。

【0057】また、本発明の受信装置は、パラメータ受信部と、をさらに備え、以下のように構成することができる。

【0058】すなわち、パラメータ受信部は、拡散符号 $z[1]$ ,  $z[2]$ , ...,  $z[L]$ を受信する。

【0059】一方、出力装置は、受信された拡散符号 $z[1]$ ,  $z[2]$ , ...,  $z[L]$ を系列初期値として受け付ける。

【0060】本発明の第4の観点に係る通信システムは、上記の送信装置と、上記の受信装置と、を備え、受信装置は、送信装置から送信された拡散符号 $z[1]$ ,  $z[2]$ , ...,  $z[L]$ を受信し、受信装置は、送信装置から送信された信号を受信するように構成する。

【0061】本発明の第5の観点に係る通信システムは、上記の送信装置と、上記の受信装置と、を備え、送信装置は、受信装置から送信された拡散符号 $z[1]$ ,  $z[2]$ , ...,  $z[L]$ を受信し、受信装置は、送信装置から送信された信号を受信するように構成する。

【0062】本発明の第6の観点に係る所定の実インパルス定数 $r$  ( $-1 < r < 1$ )と、所定の実数定数 $C$  ( $C \neq 0$ )と、に対するフィルタ装置は、入力端子と、遅延部と、増幅部と、加算部と、出力端子と、を備え、以下のように構成する。

【0063】すなわち、入力端子は、チップ長 $D$ の入力信号の入力を受け付ける。

【0064】一方、遅延部は、入力を受け付けられた入力信号を、それぞれ $0$ 、 $D$ 、 $2D$ 、 $3D$ 、...、 $(N-1)D$ だけ遅延させた複数の信号を出力する。

【0065】さらに、増幅部は、遅延されて出力された複数の信号のそれぞれを、当該遅延時間が $T$ である場

合、 $C(-r)^{1+T/D}$ 倍して出力する。

【0066】そして、加算部は、増幅されて出力された複数の信号の総和を出力する。

【0067】一方、出力端子は、加算されて出力された信号を出力する。

【0068】また、本発明のフィルタ装置において、所定の実インパルス定数 $r$ は、[数8]を満足するように構成することができる。

【0069】また、本発明のフィルタ装置において、遅延部、増幅部、および、加算部は、ASIC (Application Specific Integrated Circuit)、DSP (Digital Signal Processor)、もしくは、FPGA (Field Programmable Gate Array) によって構成されるように構成することができる。

【0070】本発明の第7の観点に係る出力方法は、所定の実インパルス定数 $r$  ( $-1 < r < 1$ )と、所定の実数定数 $C$  ( $C \neq 0$ )と、に対して、長さ $N$  ( $N \geq 1$ )の擬似乱数列を出力し、系列受付工程と、計算工程と、出力工程と、を備え、以下のように構成する。

【0071】すなわち、系列受付工程では、系列初期値として長さ $L$  ( $L \geq 1$ )の拡散符号 $z[1]$ ,  $z[2]$ , ...,  $z[L]$ の入力を受け付ける。

【0072】一方、計算工程では、入力を受け付けた $z[1]$ ,  $z[2]$ , ...,  $z[L]$ から、所定の整数 $M$  ( $1 \leq M \leq N, M+N < L$ )に対して[数10]を満たす $z'[1]$ ,  $z'[2]$ , ...,  $z'[N]$ を計算する。

【0073】さらに、出力工程では、 $z'[1]$ ,  $z'[2]$ , ...,  $z'[N]$ を擬似乱数列として出力する。

【0074】また、本発明の出力方法において、長さ $L$ の拡散符号は、 $M$ 系列、ゴールド符号、嵩符号、ウォルシュ-アダマール直交符号、もしくは、チェビシェフ多項式により生成されるカオス符号であるように構成することができる。

【0075】また、本発明の出力方法において、所定の実インパルス定数 $r$ は、[数8]を満足するように構成することができる。

【0076】本発明の第8の観点に係る送信方法は、信号受付工程と、生成工程と、拡散工程と、信号送信工程と、を備えるように構成する。

【0077】ここで、信号受付工程では、伝送信号の入力を受け付ける。

【0078】一方、生成工程では、上記の出力方法により、長さ $N$ の擬似乱数列を出力して生成する。

【0079】さらに、拡散工程では、入力を受け付けられた伝送信号を、生成された長さ $N$ の擬似乱数列を拡散符号として、スペクトラム拡散する。

【0080】そして、信号送信工程では、スペクトラム拡散された結果の信号を送信する。

【0081】また、本発明の送信方法は、選択工程と、パラメータ送信工程をさらに備え、以下のように構成す

ることができる。

【0082】すなわち、選択工程では、拡散符号 $z[1]$ 、 $z[2]$ 、 $\dots$ 、 $z[L]$ を選択する。

【0083】一方、パラメータ送信工程では、選択された拡散符号 $z[1]$ 、 $z[2]$ 、 $\dots$ 、 $z[L]$ を送信する。

【0084】さらに、生成工程では、選択された拡散符号 $z[1]$ 、 $z[2]$ 、 $\dots$ 、 $z[L]$ を系列初期値として受け付ける。

【0085】また、本発明の送信方法は、パラメータ受信工程をさらに備え、以下のように構成することができる。

【0086】すなわち、パラメータ受信工程では、拡散符号 $z[1]$ 、 $z[2]$ 、 $\dots$ 、 $z[L]$ を受信する。

【0087】一方、生成工程では、受信された拡散符号 $z[1]$ 、 $z[2]$ 、 $\dots$ 、 $z[L]$ を系列初期値として受け付ける。

【0088】本発明の第9の観点に係る受信方法は、信号受信工程と、生成工程と、逆拡散工程と、出力工程と、を備え、以下のように構成する。

【0089】すなわち、信号受信工程では、信号を受信する。

【0090】一方、生成工程では、上記の出力方法により、長さ $N$ の擬似乱数列を出力する。

【0091】さらに、逆拡散工程では、受信された信号を、出力された長さ $N$ の擬似乱数列を拡散符号として、スペクトラム逆拡散する。

【0092】そして、出力工程では、スペクトラム逆拡散された結果の信号を伝送信号として出力する。

【0093】また、本発明の受信方法は、選択工程と、パラメータ送信工程と、をさらに備え、以下のように構成することができる。

【0094】すなわち、選択工程では、拡散符号 $z[1]$ 、 $z[2]$ 、 $\dots$ 、 $z[L]$ を選択する。

【0095】一方、パラメータ送信工程では、選択された拡散符号 $z[1]$ 、 $z[2]$ 、 $\dots$ 、 $z[L]$ を送信する。

【0096】さらに、生成工程では、選択された拡散符号 $z[1]$ 、 $z[2]$ 、 $\dots$ 、 $z[L]$ を系列初期値として受け付ける。

【0097】また、本発明の受信方法は、パラメータ受信工程と、をさらに備え、以下のように構成することができる。

【0098】すなわち、パラメータ受信工程では、拡散符号 $z[1]$ 、 $z[2]$ 、 $\dots$ 、 $z[L]$ を受信する。

【0099】一方、生成工程では、受信された拡散符号 $z[1]$ 、 $z[2]$ 、 $\dots$ 、 $z[L]$ を系列初期値として受け付ける。

【0100】本発明の第10の観点に係る所定の実インパルス定数 $r$  ( $-1 < r < 1$ )と、所定の実数定数 $C$ と、に対するフィルタ方法は、入力工程と、遅延工程と、増幅工程と、加算工程と、出力工程と、を備え、以下のように構成する。

【0101】すなわち、入力工程では、チップ長 $D$ の入

力信号の入力を受け付ける。

【0102】一方、遅延工程では、入力を受け付けられた入力信号を、それぞれ $0$ 、 $D$ 、 $2D$ 、 $3D$ 、 $\dots$ 、 $(N-1)D$ だけ遅延させた複数の信号を出力する。

【0103】さらに、増幅工程では、遅延されて出力された複数の信号のそれぞれを、当該遅延時間が $T$ である場合、 $C(-r)^{1 + T/D}$ 倍して出力する。

【0104】そして、加算工程では、増幅されて出力された複数の信号の総和を出力する。

10 【0105】一方、出力工程では、加算されて出力された信号を出力する。

【0106】また、本発明のフィルタ方法において、所定の実インパルス定数 $r$ は、[数8]を満足するように構成することができる。

【0107】本発明の第11の観点に係るプログラムは、コンピュータを、上記の出力装置もしくはフィルタ装置として機能させ、または、コンピュータに上記の出力方法もしくはフィルタ方法を実行させるように構成する。

20 【0108】また、当該プログラムは、コンピュータ読取可能な情報記録媒体(コンパクトディスク、フロッピーディスク、ハードディスク、光磁気ディスク、デジタルビデオディスク、磁気テープ、または、半導体メモリを含む。)に記録することができる。

【0109】本発明の第12の観点に係るコンピュータ読取可能な情報記録媒体は、上記出力装置もしくは上記出力方法により出力される擬似乱数列を記録するように構成する。

30 【0110】本発明の情報記録媒体に記録されたプログラムを、記憶装置、計算装置、出力装置、通信装置などを備える汎用コンピュータ、携帯電話機、PHS装置、ゲーム装置などの携帯端末、並列計算機などの情報処理装置、DSP(Digital Signal Processor)、FPGA(Field Programmable Gate Array)などで実行することにより、上記の擬似乱数列の出力装置、送信装置、受信装置、通信システム、フィルタ装置にて実行される処理や、擬似乱数列の出力方法、送信方法、受信方法、ならびに、フィルタ方法を実現することができる。

40 【0111】また、これらの装置とは独立して、コンピュータ通信網を介して本発明のプログラムそのものを配布、販売したり、本発明の情報記録媒体を配布、販売することができる。

【0112】

【発明の実施の形態】以下に本発明の実施形態を説明する。なお、以下にあげる実施形態は、説明のためのものであり、本発明の範囲を制限するものではない。したがって、当業者であれば、これらの各要素または全要素を、これと均等なものに置換した実施形態を採用することが可能であるが、これらの実施形態も、本発明の範囲に含まれる。



【 0 1 1 3 】 ( 第 1 の 実 施 の 形 態 ) 図 1 は、 本 発 明 の 第 1 の 実 施 の 形 態 に 係 る 擬 似 乱 数 列 の 出 力 装 置 の 概 要 構 成 を 示 す 模 式 図 ( デ ー タ フ ロー 図 ) で 有。 以 下、 本 図 を 参 照 し て 説 明 す る。

【 0 1 1 4 】 本 実 施 形 態 に 係 る 擬 似 乱 数 列 の 出 力 装 置 1 0 1 は、 所 定 の 実 イ ン パ ル ス 定 数  $r$  ( $-1 < r < 1$ ) と、 所 定 の 実 数 定 数  $C$  ( $C > 0$ ) と、 対 して、 長 さ  $N$  ( $N > 1$ ) の 擬 似 乱 数 列 を 出 力 し、 系 列 受 付 部 1 0 2 と、 計 算 部 1 0 3 と、 出 力 部 1 0 4 と、 を 備 え る。

【 0 1 1 5 】 す な わ ち、 系 列 受 付 部 1 0 2 は、 系 列 初 期 値 と し て 長 さ  $L$  ( $L > 1$ ) の 拡 散 符 号  $z[1], z[2], \dots, z[L]$  の 入 力 を 受 け 付 け る。

【 0 1 1 6 】 一 方、 計 算 部 1 0 3 は、 入 力 を 受 け 付 け た  $z[1], z[2], \dots, z[L]$  か ら、 所 定 の 整 数  $M$  ( $1 \leq M \leq N, M + N < L$ ) 対 して [ 数 1 0 ] を 満 た す  $z'[1], z'[2], \dots, z'[N]$  を 計 算 す る。

【 0 1 1 7 】 さ ら に、 出 力 部 1 0 4 は、  $z'[1], z'[2], \dots, z'[N]$  を 擬 似 乱 数 列 と し て 出 力 す る。

【 0 1 1 8 】 計 算 部 1 0 3 に お け る 計 算 は、 コ ン ピ ュ ー タ に よ る 多 項 式 演 算 に よ り 実 現 す る こ と が 可 能 な 限 り、 加 減 算 回 路 と 乗 算 回 路 の 組 合 せ に よ っ て も 実 現 可 能。 ま た、 所 定 の 精 度 保 証 を し た 浮 動 小 数 点 演 算 で 実 現 し て も よ い し、 有 理 数 に よ る 演 算 に よ り 実 現 す る こ と も 可 能。 こ の 点 に つ い て は 後 述 す る。

【 0 1 1 9 】 ま た、 系 列 受 付 部 1 0 2 に お け る 系 列 初 期 値 お よ び 整 数 パ ラ メ ー タ の 入 力 の 受 付 や、 出 力 部 1 0 4 に お け る 出 力 は、 コ ン ピ ュ ー タ の 場 合 に は R A M ( R a n d o m A c c e s s M e m o r y ) や C P U ( C e n t r a l P r o c e s s i n g U n i t ; 中 央 処 理 ユ ニ ッ ト ) 内 の レ ジ ス タ を 介 し て 行 う こ と が 可 能、 電 子 回 路 の 場 合 に は、 ラ ッ チ な ど を 用 い て 実 現

【 0 1 2 0 】 上 記 の 漸 化 式 を 見 れ ば 明 ら か な よ う に、  $z'[1], z'[2], \dots, z'[N]$  を 各 々 求 め る た め の 計 算 は 互 い に 独 立 し て い る た め、 並 列 度 最 大  $N$  で 並 列 に 計 算 を 行 う こ と が 可 能。 ま た、 漸 化 式 で 記 述 さ れ て い る た め、 ル ー プ に よ る 繰 り 返 し 演 算 に よ っ て も 容 易 に 計 算 を 行 う こ と が 可 能。

【 0 1 2 1 】 系 列 初 期 値 と な る 拡 散 符 号 と し て は、  $M$  系 列、 ゴ ー ル ド 符 号、 嵩 符 号、 ウ ォ ル シ ュ - ア ダ マ ー ル 直 交 符 号、 も し く は、 チ ェ ビ シ ェ フ 多 項 式 に よ り 生 成 さ れ る カ オ ス 符 号 な ど を 用 い る こ と が 可 能。 以 下 で は、 チ ェ ビ シ ェ フ 多 項 式 に よ り 生 成 さ れ る カ オ ス 符 号 に つ い て 説 明 す る。

【 0 1 2 2 】 図 2 は、 チ ェ ビ シ ェ フ 多 項 式 を 表 し た グ ラ フ で 有。 チ ェ ビ シ ェ フ 多 項 式 は、 整 数  $a$  を 次 数 と す る と き、

$$T(a, \cos \theta) = \cos(a \theta)$$

の よ う に、 余 弦 関 数 の 加 法 定 理 に よ り 定 義 す る こ と が 可 能。 一 方、 以 下 の よ う に、 有 理 多 項 式 で 直 接 表 現 す る こ と も 可 能。

$$\begin{aligned} T(0, x) &= 1 \\ T(1, x) &= x \\ T(2, x) &= 2x^2 - 1 \\ T(3, x) &= 4x^3 - 3x \end{aligned}$$

【 0 1 2 3 】 チ ェ ビ シ ェ フ 多 項 式  $y = T(a, x)$  は、 い づ れ も、 開 区 間  $-1 < x < 1$  を 開 区 間  $-1 < y < 1$  に 写 像 す る 有 理 写 像 で 有。

【 0 1 2 4 】 本 図 に は、 次 数 2 か ら 5 の チ ェ ビ シ ェ フ 多 項 式 が、  $y = T(2, x), y = T(3, x), y = T(4, x), y = T(5, x)$  の 形 式 で グ ラ フ 表 示 さ れ て い る。 横 軸 が  $x$  軸、 縦 軸 が  $y$  軸 で 有。

【 0 1 2 5 】 こ の よ う な チ ェ ビ シ ェ フ 多 項 式 を 用 い て 生 成 さ れ る カ オ ス 符 号 と し て は、 以 下 の よ う な も の が 考 え ら れ る。 第 1 は、 最 も 基 本 的 な カ オ ス 符 号 で 有、 以 下 の 漸 化 式 に よ り 計 算 さ れ る も の で 有。

$$z[i+1] = T(a, z[i])$$

【 0 1 2 6 】 第 2 は、 こ れ を 応 用 し た も の で 有、 系 列 初 期 値  $Y_1, Y_2, \dots, Y_s$  ( $-1 < Y_1 < 1, -1 < Y_2 < 1, \dots, -1 < Y_s < 1$ )、 所 定 の 整 定 数  $q_1, q_2, \dots, q_s$ 、 所 定 の 整 数 パ ラ メ ー タ  $p_1, p_2, \dots, p_s$  (た だ し  $q_i \bmod p_i \neq 0, q_i \bmod p_i \neq 0, \dots, q_s \bmod p_s \neq 0$ ) 対 して 以 下 の 漸 化 式 [ 数 1 1 ] を 用 い て 計 算 さ れ る も の で 有。

【 0 1 2 7 】

【 数 1 1 】

$$\begin{aligned} y_j[1] &= Y_j \\ y_j[m+1] &= T(p_j, y_j[m]) \\ z[n] &= \prod_{j=1}^s T(q_j, y_j[n]) \end{aligned}$$

【 0 1 2 8 】 ( 理 論 的 背 景 ) チ ェ ビ シ ェ フ 多 項 式 に よ る カ オ ス 符 号 を 用 い た 場 合 に 出 力 さ れ る 長 さ  $N$  の 擬 似 乱 数 列 の 相 関 関 数 が、 上 記 の 最 適 相 関 関 数 と な る こ と は、 エ ル ゴ ー ド 理 論 に お い て 展 開 さ れ る ル ベ ー グ ス ペ ク ト ラ ム ( Lebesgue Spectrum ) の 理 論 に 基 づ く。 本 理 論 に つ い て は、 以 下 の 文 献 に 開 示 さ れ て い る。

V. I. Arnold and A. Avez 「Ergodic Problems of Classical Mechanics」

( W. A. Benjamin, New York, 1968 )

【 0 1 2 9 】 以 下、 ル ベ ー グ ス ペ ク ト ラ ム の 理 論 を 説 明 す る。

【 0 1 3 0 】 今、  $X_{n+1} = F(X_n)$  と い う 力 学 系 か ら 生 成 さ れ た 系 列  $X_1, X_2, \dots$  が、 そ の 力 学 系 を 定 義 す る 領 域  $Q$  上 の 極 限 密 度 分 布 関 数 ( 不 変 測 度 )  $\rho(x)dx$  対 して、 エ ル ゴ ー ド 性 を 持 つ と す る。

【 0 1 3 1 】 す る と、 こ の 不 変 測 度 に 関 す る 内 積

$$\langle u, v \rangle = \int_Q u(x)v(x) \rho(x)dx$$

か ら、 自 然 に ノ ル ム 演 算  $\| \cdot \|$  が

$$\|v\|^2 = \langle v, v \rangle$$

の よ う に 定 義 さ れ る ヒ ル ベ ル ト 空 間  $L_2$  を 考 え る こ と が 可

きる。

【0132】上記文献によれば、この $L_2$ 空間に、ある力学系に依存する特殊な性質を満足する正規直交基底 [数12] が一意的に存在する。これをルベークスペクトラムと呼ぶ。

【0133】

【数12】

$$\{\phi_{\lambda,j}\}_{\lambda \in \Lambda, j \in \mathcal{J}}$$

【0134】ここで、 $\phi_{\lambda,j}$  は、このルベークスペクトラムの各クラスをラベル付けするものであり、 $j$  は、その各クラスの関数を指し示すラベルで加算無限個ある0以上の整数に対応する。

$$\phi_{\lambda,j} \circ F(x) = \phi_{\lambda,j+1}(x)$$

【0138】即ち、もし、以下の関数 [数14] が与えられれば、クラス  $\phi_{\lambda,0}$  の他のルベークスペクトラム関数 [数15] は、すべて、力学系を定義する写像 $F(\cdot)$ を繰り返し、適用することにより得ることができる。

【0139】

【数14】

$$\phi_{\lambda,0}$$

【0140】

【数15】

$$\{\phi_{\lambda,j}\}_{j \geq 1}$$

【0141】また、ルベークスペクトラムが正規直交系を成すという仮定により、これらの各関数 [数16] は、同一のクラスの任意の他の関数 [数17] および、任意の他のクラスの任意の関数 [数18] と直交する。

【0142】

【数16】

$$\phi_{\lambda,j}$$

【0143】

【数17】

$$\phi_{\lambda,j'}$$

【0144】

【数18】

$$\phi_{\lambda',j''}$$

【0145】完全なルベークスペクトラムを持つエルゴ

$$\overline{B(x)B(F^l(x))} = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N B(X_n)B(X_{n+l})$$

【0153】各 $X_n$  は、漸化式 $X_{n+1} = F(X_n)$ により生成され、この時間平均が空間平均に等しいというエルゴード等式は、 $Q$ 上の測度0の例外的初期値 $X_1$ を除いて成立す

10

20

30

40

50

【0135】この定義から、ルベークスペクトラムは、無限個の関数からなる正規直交関数系であることがわかる。特に、ラベル  $\phi_{\lambda,j}$  のとりうる種類の数 (  $\phi_{\lambda,j}$  の cardinality ) が無限の場合、このルベークスペクトラムを無限ルベークスペクトラムと呼ぶ。また、このルベークスペクトラムが、正規直交基底だけでなく、 $L_2$ 空間において完全正規直交基底である場合には、このルベークスペクトラムを完全ルベークスペクトラムと呼ぶ。

【0136】さて、上述のルベークスペクトラムの持つ特殊な性質とは、以下を満足することである。

【0137】

【数13】

$$(\text{for } \forall \lambda \in \Lambda, \forall j \in \mathcal{J})$$

ード力学系として、後で述べる2次以上のチェビシェフ多項式で与えられるチェビシェフカオス力学系がある。チェビシェフカオス力学系については、以下の文献に開示されている。

R. L. Adler, T. J. Rivlin 「Proc. Am. Math. Soc. 15」 (1964, p794)

【0146】今、 $L_2$ のある関数 $B(x)$ が、 [数19] のようにルベークスペクトラムで展開できるとする。

【0147】

【数19】

$$B(x) = \sum_{j=1}^M a_{\lambda,j} \phi_{\lambda,j}(x)$$

【0148】この場合、相関関数 [数20] は、ルベークスペクトラムの直交性から、 [数21] のように、ルベークスペクトラム展開係数により与えられる。

【0149】

【数20】

$$\langle B(x), B(F^l(x)) \rangle \equiv \langle B_0, B_l \rangle$$

【0150】

【数21】

$$\langle B_0, B_l \rangle = \sum_{m=l+1}^{M+l} a_{\lambda,m} a_{\lambda,m-l}$$

【0151】なお、この相関関数は、エルゴード性により、時間平均 [数22] に等しい。

【0152】

【数22】

る。

【0154】今、ここで、以下のように仮定する。

【0155】

【数 2 3】

$$a_{\lambda,m} = C_0(-r)^{M+1+l-m} \quad (m = 1, 2, \dots, M)$$

【0 1 5 6】ただし  $C_0$  は 0 でない定数である。これを、上の相関関数を与える式に代入すると、[数 2 4] が得られ、相関関数は、[数 2 5] のように、指数関数的に減少する。

$$\langle B_0, B_l \rangle = C_0^2(-r)^l \frac{1 - r^{2M}}{1 - r^2}$$

【0 1 5 7】

【0 1 5 8】

【数 2 4】

【数 2 5】

$$C(l) \equiv \langle B_0, B_l \rangle = C'(-r)^l \quad (M \rightarrow \infty)$$

【0 1 5 9】このように、符号シフト量  $l$  に関して、 $(-r)^l$  の形で指数関数的にダンプする相関関数を持つ系列を、任意の  $r$  ( $-1 < r < 1$ ) に対して、自由自在に、作ることができる。

【0 1 6 1】干渉ノイズの分散が、[数 9] となるような拡散系列は、その相関関数の漸近的振る舞いが、[数 7] のようになればよい。したがって、ルベグスペクトラムを持つエルゴード力学系と、そのルベグスペクトラム関数により定義される上述の  $B(x)$  で、[数 2 6] のように設計されるフィルタを用意すれば十分である。

【0 1 6 0】特に、Mazzini が発見したように、ランダム符号 (ゴールド符号、嵩符号も含む) を拡散系列とした時よりも、同一ビット誤り率下で、[数 1 0] の場合、15 パーセント理論的ユーザ数を増やすことができる。

【0 1 6 2】

【数 2 6】

$$a_{\lambda,m} = C(-r)^{M+1-m}$$

$$r = 2 - \sqrt{3} \quad (m = 1, 2, \dots, M)$$

【0 1 6 3】さて、ここで問題となるのは、どのようにすれば、エルゴード力学系  $F(x)$  とルベグスペクトラム [数 1 2] とを実現容易な形で構成できるかということである。以下では、チェビシェフ写像による構成について説明する。

$$\int_Q T_p(x) T_q(x) \rho(x) dx = 0 \quad (\text{for } q \neq p)$$

【0 1 6 4】今、2 次以上のチェビシェフ多項式  $T_p(x)$  ( $p \geq 2$ ) を考える。このチェビシェフ多項式は、上述のように、 $T_p(\cos \theta) = \cos(p \theta)$  のように定義され、それぞれの  $p$  の値に対して、閉区間  $Q = [-1, 1]$  上の分布関数 [数 2 7] の下で、[数 2 8] のように直交することが知られている。

【0 1 6 7】これらのチェビシェフ多項式と分布関数により、ヒルベルト空間  $L_2$  を構成することができる。この場合、チェビシェフ多項式は、ヒルベルト空間  $L_2$  における完全性を持つ直交基底となる。

【0 1 6 5】

【数 2 7】

$$\rho(x) dx = \frac{dx}{\pi \sqrt{1 - x^2}}$$

【0 1 6 8】また、上述の文献には、2 つ以上のチェビシェフ写像で与えられる力学系が、エルゴード性を有するほか、これよりも強い混合性という性質を持つことが開示されている。この場合のエルゴード的な不変測度は、上述の直交性を定義する密度関数  $\rho(x)$  により与えられる。

【0 1 6 6】

【数 2 8】

$$\phi_{q,j}(x) = T_{qpj}(x) \quad (j \geq 0, q(\text{mod } p) \neq 0)$$

【0 1 7 1】すると、チェビシェフ多項式自身の直交性と、関係式 [数 3 0] とから、関数系  $\phi_{q,j}(x)$  はルベグスペクトラムであることがわかる。

【0 1 7 0】

【数 2 9】

$$\phi_{q,j} \circ T_p(x) = T_{qpj} \circ T_p(x) = T_{qpj+1}(x) = \phi_{q,j+1}(x)$$

【0 1 7 3】したがって、整数  $M$  ( $1 \leq M \leq N$ ) に対して、[数 3 1] のようにフィルタを設計すれば、上述のルベ

【0 1 6 9】これらの性質から、今、[数 2 9] のように関数系  $\phi_{q,j}(x)$  を定義する。

40

【0 1 7 2】  
【数 3 0】  
—グスペクトラム理論の相関関数の明示解により、相関関数 [数 7] を持つ非同期 CDMA 通信システム用の拡

50

散符号を構成することができる。これは、上述のように、Mazziniの理論により示されたものであり、通常のランダム符号を基礎とする非同期CDMAのある一定のビット誤り率のもとでのユーザー数を、15パーセント

$$B(x) = C \sum_{j=1}^M (-r)^{M+1-j} \phi_{q,j}(x) \quad (r = 2 - \sqrt{3})$$

【0175】ここで、[数32][数33]が成立し、任意の整数m (0 ≤ m ≤ N-1)に対して[数34][数35]であることに着目する。

【0176】

【数32】

$$\begin{aligned} B(X_1) &= C \sum_{j=1}^M (-r)^{M+1-j} \phi_{q,j}(X_1) \\ &= C \sum_{j=1}^M (-r)^{M+1-j} \phi_{q,0}(X_{1+j}) \end{aligned}$$

【0177】

【数33】

$$B(X_1) = C \sum_{j=1}^M (-r)^{M+1-j} T_q(X_{1+j})$$

【0178】

【数34】

$$\begin{aligned} B(X_m) &= C \sum_{j=1}^M (-r)^{M+1-j} \phi_{q,j}(X_m) \\ &= C \sum_{j=1}^M (-r)^{M+1-j} \phi_{q,0}(X_{m+j}) \end{aligned}$$

【0179】

【数35】

$$B(X_m) = C \sum_{j=1}^M (-r)^{M+1-j} T_q(X_{m+j})$$

【0180】この関数B(x)は、q=1の場合、T<sub>q</sub>(x) = xとなり、[数36]が成立する。

【0181】

【数36】

$$B(X_m) = C \sum_{j=1}^M (-r)^{M+1-j} X_{m+j}$$

【0182】これは、系列X<sub>m+1</sub>, X<sub>m+2</sub>, ..., X<sub>m+j</sub>, ..., X<sub>m+M-1</sub>, X<sub>m+M</sub> (1 ≤ j ≤ M)を、それぞれ、C(-r)<sup>M+1-j</sup>に与えられる定数により定数倍した結果の和をとる操作を意味する。

【0183】これは、デジタル信号処理の基本フィルタの一つであるFIRフィルタ(Finite Impulse Response Filter)の操作に他ならない。

増加することができる。

【0174】

【数31】

【0184】よって、既存のDSP技術によって本発明に係る計算を、本FIRフィルタにより実現する高速かつ低消費電力のデバイスが構成できる。

10 【0185】図3は、このようにして構成したフィルタの概要構成を示す模式図である。

【0186】フィルタ301は、チェビシェフ・カオス型の拡散符号系列など、各種の拡散符号系列X<sub>1</sub>, X<sub>2</sub>, X<sub>3</sub>, ...の入力を、端子305にて受け付ける。

【0187】受け付けられた拡散符号系列は、直列接続された遅延回路302により、順次遅延されて配送される。遅延時間は、チップ長である。

20 【0188】また、遅延回路302同士の間順次現れる拡散符号を、増幅器303によって増幅する。本図には、所定の実数定数C=1の場合を示しており、増幅率は、それぞれ、(-r)<sup>1</sup>, (-r)<sup>2</sup>, (-r)<sup>3</sup>, ..., (-r)<sup>M-1</sup>, (-r)<sup>M</sup>である。

【0189】なお、増幅器303のそれぞれの増幅率は、一般には、所定の実数定数Cに対して、それぞれ、C(-r)<sup>1</sup>, C(-r)<sup>2</sup>, C(-r)<sup>3</sup>, ..., C(-r)<sup>M-1</sup>, C(-r)<sup>M</sup>とすることになる。

30 【0190】ここで、rを[数8]にて定義される実インパルス定数とした場合が最適となるが、[数8]を厳密に満足しなくとも、-1 < r < 1である限り、非同期CDMA通信システムの拡散符号生成に用いることができる。

【0191】増幅器303によって増幅された信号は、加算器304によって加算され、擬似乱数列Y<sub>1</sub>, Y<sub>2</sub>, Y<sub>3</sub>, ...が順次出力される。

【0192】なお、拡散符号としてチェビシェフ多項式を用いて生成されるカオス符号を用いた場合は、符号系列を周期的にすることができる。

40 【0193】すなわち、X<sub>j</sub> = X<sub>j+N+1</sub>である場合は、2N-1個の数値X<sub>1</sub>, ..., X<sub>2N-1</sub>を用意する必要はない。N個のX<sub>1</sub>, ..., X<sub>N</sub>だけあれば、周期性を利用して、すべてのm (0 ≤ m ≤ N)に対して、B(X<sub>m</sub>)を計算できる。したがって、さらに計算時間を短縮することができる。

【0194】同様に、チェビシェフ多項式の積[数37]もs次元キュービック[-1, 1]<sup>s</sup>上で、完全直交基底となることが解る。

【0195】

【数37】

$$T_{p_1}(x_1) T_{p_2}(x_2) \cdots T_{p_s}(x_s)$$

【 0 1 9 6 】本実施形態では、s個の所定の正整数 $q_1, q_2, \dots, q_s$ に対して、それぞれ $q_1 \bmod p_1 = 0, q_2 \bmod p_2 = 0, \dots, q_s \bmod p_s = 0$ が成立するようなs個の整数パラメータ $p_1, p_2, \dots, p_s$ で決められるチェビシェフ写像力学系から、それぞれ生成されたs次元の実数

$$z[m] = T_{q_1}(x_1[m])T_{q_2}(x_2[m]) \cdots T_{q_s}(x_s[m])$$

$$(1 \leq m \leq 2N - 1)$$

【 0 1 9 8 】すると、計算された値 $z[1], z[2], \dots, z[2N-1]$ から構成される長さNの擬似拡散系列 [ 数 3 9 ] の相関関数は、[ 数 7 ]を満足する。

【 0 1 9 9 】

【 数 3 9 】

$$z'[1] = C \sum_{j=1}^M (-r)^{M+1-j} z[j],$$

$$z'[2] = C \sum_{j=1}^M (-r)^{M+1-j} z[j + 1],$$

$$\vdots$$

$$z'[N] = C \sum_{j=1}^M (-r)^{M+1-j} z[j + N - 1]$$

【 0 2 0 0 】よって、[ 数 8 ]のようにrを定義し、符号長Nを十分に長くすれば、s次元の直積カオス力学系から作られる擬似乱数列を拡散符号とする非同期CDMAの干渉ノイズの分散は、上記Mazziniの理論により [ 数 9 ]によって表され、既存の非同期CDMA通信システムの場合より、同一ビット誤り率下で確実に15パーセントのユーザー数を増やすことができる。

【 0 2 0 1 】また、チェビシェフ写像 $T_p(x)$ と、微分同相写像 $G(x)$ に対して、[ 数 4 0 ]の関係 (位相同型)を満足すれば、この $F_p(x)$ も、チェビシェフ写像と同等なルベグスペクトラムを持ち、更に、本自己相関関数が、 $(-r)^j$ の様にダンプする様なカオス系列を、同様に構成することができる。

【 0 2 0 2 】

【 数 4 0 】

$$F_p \circ G(x) = G \circ T_p(x)$$

【 0 2 0 3 】(実験結果)以下では、擬似乱数列の長さNを固定して、ユーザー数Kならびにタップ数Mに対して、本手法のビット誤り率を計算したシミュレーション結果を示す。与える拡散符号は、チェビシェフ符号、ゴールド符号、ならびに、一般的なランダム列である。なお、本手法では、以下のパラメータを用いた。

- ・s=1。
- ・p=2 (チェビシェフGeneratorの次数は、2に相当)。

【 0 2 0 4 】図 4 から図 7 は、符号長N=31に対するもの

値 $x_1, x_2, \dots, x_s$ に対して、s個の積 [ 数 3 8 ] を計算する。

【 0 1 9 7 】

【 数 3 8 】

であり、図 8 から図 1 1 は、符号長N=63に対するものであり、図 1 2 から図 1 5 は、N=127に対するものである。

【 0 2 0 5 】これらのシミュレーション結果から、いずれの拡散符号を用いた場合であっても、従来の手法と比較して、同一ビット誤り率下で、15パーセント増のユーザー数を確保することができることがわかる。

【 0 2 0 6 】また、タップ数Mに対するビット誤り率は、M = 2~5程度で飽和していることがわかる。したがって、フィルタの段数Mは、この程度の数でよいこともわかる。

20 【 0 2 0 7 】このほか、与える拡散符号は、必ずしもチェビシェフ多項式を用いたカオス符号でなくともよいことがわかる。

【 0 2 0 8 】(出力方法の詳細)図 1 6 は、擬似乱数列の出力装置 1 0 1 において実行される処理、すなわち、本発明の擬似乱数列の出力方法の工程を示すフローチャートである。

30 【 0 2 0 9 】擬似乱数列の出力装置 1 0 1 は、系列初期値と整数パラメータ (次数) を受け付け (ステップ S 3 0 1)、これらと上記の漸化式に基づいて擬似乱数列を計算し (ステップ S 3 0 2)、計算した擬似乱数列を出力して (ステップ S 3 0 3)、本処理を終わる。

【 0 2 1 0 】このように、本発明の擬似乱数列の出力方法は、汎用コンピュータ、並列コンピュータ、携帯端末、特に通信端末、ゲーム装置などの情報処理装置により容易に実行することができる。

【 0 2 1 1 】また、DSPやFPGA (Field Programmable Gate Array) などのデジタル回路を用いて、本発明の擬似乱数列の出力方法を実行することも容易である。

40 【 0 2 1 2 】(送信装置の実施形態)図 1 7 は、本発明の送信装置の概要構成を示す模式図である。なお、上記の図と同じ要素には、同じ符号を付してある。以下、本図を参照して説明する。

【 0 2 1 3 】送信装置 4 0 1 は、信号受付部 4 0 2 と、系列出力部 4 0 3 と、拡散部 4 0 4 と、信号送信部 4 0 5 と、を備える。系列出力部 4 0 3 は、擬似乱数列の出力装置 1 0 1 を備えており、これを制御する。

【 0 2 1 4 】信号受付部 4 0 2 は、伝送すべき信号を受け付ける。伝送信号として典型的なものは、携帯電話やPHSの場合には音声信号である。デジタル通信を行

う場合には、電気的なデジタル信号である。光通信を行う場合には、光信号から電気信号への変換を行った上で電気信号を受け付けてもよいし、擬似乱数列の出力装置 101 を光コンピュータで実現する場合は、光信号をそのまま受け付ける。

【0215】系列出力部 403 は、送信装置 401 に割り当てられた系列初期値と整数パラメータ（次数）とを、これが備える擬似乱数列の出力装置 101 に受け付けさせる。擬似乱数列の出力装置 101 は、上述のように、擬似乱数列を出力するので、系列出力部 403 は、この擬似乱数列を出力する。

【0216】系列初期値と整数パラメータ（次数）とは、送信装置 401 のそれぞれに異なる値をあらかじめ割り当てることができる。製造番号、機器番号、承認番号などの数値を ROM（Read Only Memory）に記録した通信端末が普及しているが、これと同様に、系列初期値と整数パラメータ（次数）とをあらかじめ ROM に記録しておいて、当該送信装置 401 が常に同じ系列初期値と整数パラメータ（次数）とを用いるようにすることができる。また、ROM 内に使用する系列初期値と整数パラメータ（次数）とを複数の種類記録しておき、これら

を通信ごとにランダムに選択する手法も利用できる。【0217】このような実施形態をとる場合、送信装置 401 と通信する受信装置では、ROM 内に記録された系列初期値と整数パラメータ（次数）とを何らかの方法で知る必要があるが、送信装置と受信装置とが 1 対になっている場合には、同じ系列初期値と整数パラメータ（次数）とを共有して記録する実施形態をとることができる。

【0218】系列初期値と整数パラメータ（次数）の種類が複数ある場合に、送信装置 401 がいずれを使用しているか、は、後述する相関検波によって調べることができる。また、チェビシェフ多項式に基づく漸化式によって得られるカオス乱数列を用いて系列初期値を複数用意してもよい。さらに、後述するように、公開鍵暗号の手法を用いて、送信装置 401 と受信装置とで系列初期値と整数パラメータ（次数）を安全に共有することができる。

【0219】拡散部 404 は、信号受付部 402 が受け付けた伝送信号に、系列出力部 403 が出力した擬似乱数列の要素を順に乗じて直接スペクトラム拡散する。ここで、時刻  $t$  における信号の値を  $s(t)$  として、「信号  $s(t)$  に系列の要素を順に乗じる」手法について説明する。

【0220】長さ  $N$  の系列の要素を用いる場合には、これと直接スペクトラム拡散のチップ長  $w$  から、「信号  $s(t)$  に系列の要素を順に乗じる」の周期は、 $Nw$  になる。

【0221】所定の時刻  $t_0$  から「信号  $s(t)$  に系列の要素を順に乗じる」場合、信号  $s(t)$  を、必要な品質が得られるようなチップ長  $w$  で離散化する。たとえば、チップ長  $w$

ごとに信号  $s(t)$  の値を得る手法や、チップ長  $w$  の間の信号  $s(t)$  の値の平均を得る手法などが考えられる。ここでは、説明を明確にするため、前者の手法を用いて説明する。

【0222】チップ長  $w$  は、受信装置側で伝送信号の情報を必要な品質で十分に復号できるような長さにする必要があるが、公知の技法により、適切なチップ長を選択することができる。

【0223】また、適切なチップ長  $w$  を選択すれば、離散化された信号列を順に当該チップ長時間  $w$  だけ出力することにより、元の伝送信号から見て十分な品質の信号を得ることができる。

【0224】離散化された信号は、以下のような数列で表現することができる。

$$s(t_0), s(t_0+w), s(t_0+2w), s(t_0+3w), s(t_0+4w), \dots$$

【0225】これは、整数  $i$  ( $0 \leq i$ ) について

$$s_i = s(t_0+iw)$$

と整理することができる。

【0226】なお、チップ長  $w$  の間の信号  $s(t)$  の値の平均をとる手法では、以下のように整理することができる。

$$s_i = (1/w) \int_0^w s(t_0+iu) du$$

【0227】これらの信号列  $s_i$  ( $0 \leq i$ ) は、必要な品質で伝送信号を離散化したものである。

【0228】この信号列を、直接スペクトラム拡散した後の信号列は、

$$s_0 z^{-1}[1], s_1 z^{-1}[2], \dots, s_{N-1} z^{-1}[N], s_N z^{-1}[1], s_{N+1} z^{-1}[2], \dots$$

のようになる。

【0229】すなわち、整数  $i$  ( $0 \leq i$ ) に対して、 $s_i \times z^{-1}[(i \bmod N)+1]$  が、この数列の一般項である。ここで、 $x \bmod y$  は、 $x$  を  $y$  で割った余りを意味する。

【0230】この信号列の要素を、それぞれチップ長の時間だけ送信することにより、受け付けられた所定の時間長の伝送信号を同じ時間長で送信することができる。

【0231】図 18 には、直接スペクトラム拡散処理の様子を示す。信号受付部 402 が受け付けた伝送信号 501 に対して、系列出力部 403 が出力した擬似乱数列 502 の要素を繰り返し乗ずることにより、拡散部 404 が出力する信号 503 が得られる。

【0232】信号送信部 405 は拡散部 404 が出力する信号 503 を送信する。送信は、たとえば、携帯電話や PHS の場合はアンテナを介して、コンピュータ通信網の場合は有線の電話回線や有線/無線 LAN 回線を介して、あるいは光ケーブルを介して行われる。

【0233】（受信装置の実施形態）本発明の受信装置は、上記の送信装置同様、上記の擬似乱数列の出力装置を用いて擬似乱数列を得て、これを直接スペクトラム逆拡散用の拡散符号として用いる。図 19 は、本発明の受信装置の概要構成を示す模式図である。以下、本図を参

照して説明する。

【0234】受信装置601は、信号受信部602と、系列出力部604と、逆拡散部605と、を備える。

【0235】信号受信部602は、上記の送信装置401により送信された信号を受信する。信号受信部602は、たとえば、アンテナ、電話回線や光ケーブル回線などに対するインターフェースにより実現される。

【0236】信号受信部602が受信する信号には、通信相手以外の送信装置401が送信した信号や、ノイズが含まれている。これら不要な信号を除去するために、通信相手の送信装置401が直接スペクトラム拡散に用いた擬似乱数列と同じ擬似乱数列を用いる。系列出力部604は、通信相手の送信装置401が用いた系列初期値と整数パラメータ（次数）と、を上記の擬似乱数列の出力装置101に受け付けさせることにより、この擬似乱数列を出力する。したがって、受信装置601の系列出力部604の実施態様は、送信装置401の系列出力部403と同様である。

【0237】通信相手の送信装置401が受け付けた伝送信号を復号するには、通信相手の送信装置401が送信した信号に対して、擬似乱数列の要素の逆数を順に乗じて直接スペクトラム逆拡散すればよい。

【0238】同期が取れていれば、逆拡散部605において、受信した信号列

$$s_0 z'[1], s_1 z'[2], \dots, s_{N-1} z'[N], s_N z'[1], s_{N+1} z'[2], \dots$$

に、擬似乱数列の要素の逆数

$$1/z'[1], 1/z'[2], \dots, 1/z'[N]$$

を順に乗ずることにより、伝送信号の情報を必要な品質で復号した信号列

$$s_0, s_1, \dots, s_{N-1}, s_N, s_{N+1}, \dots$$

が得られる。この信号列を、それぞれチップ長時間 $w$ だけ順に出力すれば、伝送信号が必要な品質で復元できるのである。

【0239】同期には、後述する相関検波のほか、クロックを共有する手法など、各種の手法が考えられ、これらの実施形態も本発明の範囲に含まれる。

【0240】以下のように、送信装置401と受信装置601とで通信を行う公開鍵暗号の手法を用いて、受信装置の生成部611は、送信装置401と同じ系列初期値および整数パラメータ（次数）を生成することができる。

【0241】まず、受信装置601は、公開鍵と秘密鍵の対を生成する。次に、受信装置601は、送信装置401に対して公開鍵を送信する。送信装置401は、自ら使用する系列初期値および整数パラメータ（次数）を当該公開鍵で暗号化して受信装置601に送信する。受信装置601は、送られた暗号を秘密鍵で復号し、系列初期値および整数パラメータ（次数）を得る。

【0242】このような公開鍵暗号の手法として、本発

明の発明者が特願平11-152063号に開示するようなカオス暗号を用いることができる。

【0243】（拡散・逆拡散の他の実施形態）上記の実施形態のほか、拡散・逆拡散の際に、以下の実施形態を採用することもできる。すなわち、それぞれが+1もしくは-1の値をとる以下の情報データを伝送したい場合を考える。

$$b_1, b_2, b_3, \dots$$

10 【0244】送信装置401では、この系列に、以下のように擬似乱数列を順に乗じる。

$$b_1 z'[1], b_1 z'[2], \dots, b_1 z'[N],$$

$$b_2 z'[1], b_2 z'[2], \dots, b_2 z'[N],$$

$$b_3 z'[1], b_3 z'[2], \dots, b_3 z'[N], \dots$$

【0245】送信装置401は、この拡散済み信号を伝送する。

【0246】一方、受信装置601が受信した信号が以下の通りだったとする。

$$s_1, s_2, \dots, s_N,$$

$$s_{N+1}, s_{N+2}, \dots, s_{2N},$$

20  $s_{2N+1}, s_{2N+2}, \dots, s_{3N}, \dots$

【0247】受信装置601では、これに擬似乱数列を順に乘じ、 $N$ 個ごとに和をとる。すなわち、以下のようにして逆拡散を行う。

$$e_1 = s_1 z'[1] + s_2 z'[2] + \dots + s_N z'[N],$$

$$e_2 = s_{N+1} z'[1] + s_{N+2} z'[2] + \dots + s_{2N} z'[N],$$

$$e_3 = s_{2N+1} z'[1] + s_{2N+2} z'[2] + \dots + s_{3N} z'[N], \dots$$

【0248】このようにして得られた系列が、復元された情報データである。

【0249】なお、この手法においては、当初の情報データ $b_1, b_2, b_3, \dots$ の $N$ 倍の数のデータが送信装置401から送信される。受信装置601では、復元された情報データ $e_1, e_2, e_3, \dots$ の数は、受信したデータの数の $1/N$ となる。したがって、送信ならびに受信される信号のチップ長を $w$ とすると、当初の情報データならびに復元された情報データのチップ長は $Nw$ となる。

【0250】上記の計算は内積に相当するが、拡散符号が互いに直交するため、内積をとることにより、他のユーザの送信信号の振幅を零にすることができる。したがって、必要な信号のみを取得することができる。

40 【0251】（相関検波の実施形態）送信装置401で、複数の擬似乱数列からいずれかを選択して直接スペクトラム拡散した場合、受信装置601は、相関検波により、選択された擬似乱数列を知得することができる。また、相関検波により、直接スペクトラム逆拡散のための同期をとることができる。

【0252】以下、図20を参照して、相関検波を行う場合の受信装置の実施形態について説明する。なお、図20では、上記の図に示す要素と同じものには同じ符号を付している。

50 【0253】受信装置601は、信号受信部602と、

系列出力部 604 と、逆拡散部 605 と、のほか、生成部 611 と、相関検波部 612 を備える。

【0254】生成部 611 は、送信装置 401 で選択可能な系列初期値と整数パラメータ（次数）の組を出力する。擬似乱数列を 1 つだけ出力してもよい。この場合、相関検波部 612 は、複数の系列初期値と整数パラメータ（次数）の組からいずれか 1 つの組を選択する必要はないため、信号の同期をとるために機能する。

【0255】系列出力部 604 は、生成部 611 が生成する系列初期値と整数パラメータ（次数）に応じて、送信装置 401 で選択可能な擬似乱数列をそれぞれ出力する。

【0256】相関検波部 612 では、系列出力部 604 が出力する擬似乱数列のそれぞれについて相関検波を試みる。調べたい擬似乱数列の「要素」を順に受信した信号に乗ずることにより、相関検波を行う。相関検波の手法については公知の技法を用いることができる。

【0257】本発明で用いる擬似乱数列は、相関特性に優れているため、受信装置 601 で異なる擬似乱数列を選択した場合には、乗じた後の信号の強度が極めて弱くなり、相関検波に失敗する。

【0258】一方、送信装置 401 の擬似乱数列と同じものを選択して相関検波を行った場合は、乗じた後の信号の強度が所定の値を超えることになる。また、受信信号に同期するように擬似乱数列のオフセットを移動して信号の同期をとることができる。

【0259】逆拡散部 605 は、信号受信部 602 により受信された信号に、相関検波部 612 により選択されて当該受信された信号に同期された擬似乱数列の「要素の逆数」を順に乗じて、伝送信号を復号する。

【0260】受信された信号に対して、相関検波部 612 では擬似乱数列の「要素」を順に乗ずるのに対し、逆拡散部 605 では擬似乱数列の「要素の逆数」を順に乗ずる点異なる。前者では、自己相関、相互相関を計算するのに対し、後者では、復号が行われるのである。

【0261】（通信システム）本発明の通信システムは、上記の送信装置 401 と、これが送信する信号を受信して伝送信号を復号する上記の受信装置 601 と、から構成することができる。これらの送信装置 401 と受信装置 601 で、使用する擬似乱数列が異なれば伝送信号の復号に失敗する。

【0262】したがって、複数の送信装置 401 と複数の受信装置 601 とが同じ周波数帯で通信していても、秘話性を保つとともに、使用している通信者の対の数に応じた品質を保証して、相互に通信を行うことができる。

【0263】特に、本発明にて生成される擬似乱数列では、従来の擬似乱数列に比較して符号の種類を格段に増やすことができるため、潜在的に多数のユーザを含むような CDMA 方式の通信に適している。

【0264】

【発明の効果】以上説明したように、本発明によれば、非同期 CDMA 通信システムにて拡散符号として用いるのに好適な擬似乱数列の出力装置、送信装置、受信装置、通信システム、フィルタ装置、擬似乱数列の出力方法、送信方法、受信方法、フィルタ方法、ならびに、情報記録媒体を提供することができる。

【図面の簡単な説明】

10 【図 1】本発明の擬似乱数列の出力装置の概要構成を模式図である。

【図 2】チェビシェフ写像の概要を示すグラフである。

【図 3】本実施形態にて利用可能な FIR フィルタの概要構成を示す模式図である。

【図 4】本手法のビット誤り率のシミュレーション結果を示すグラフである。

【図 5】本手法のビット誤り率のシミュレーション結果を示すグラフである。

【図 6】本手法のビット誤り率のシミュレーション結果を示すグラフである。

20 【図 7】本手法のビット誤り率のシミュレーション結果を示すグラフである。

【図 8】本手法のビット誤り率のシミュレーション結果を示すグラフである。

【図 9】本手法のビット誤り率のシミュレーション結果を示すグラフである。

【図 10】本手法のビット誤り率のシミュレーション結果を示すグラフである。

【図 11】本手法のビット誤り率のシミュレーション結果を示すグラフである。

30 【図 12】本手法のビット誤り率のシミュレーション結果を示すグラフである。

【図 13】本手法のビット誤り率のシミュレーション結果を示すグラフである。

【図 14】本手法のビット誤り率のシミュレーション結果を示すグラフである。

【図 15】本手法のビット誤り率のシミュレーション結果を示すグラフである。

【図 16】本発明の擬似乱数列の出力方法の工程を示すフローチャートである。

40 【図 17】本発明の送信装置の概要構成を示す模式図である。

【図 18】直接スペクトル拡散の様子を示す説明図である。

【図 19】本発明の受信装置の概要構成を示す模式図である。

【図 20】相関検波を行う場合の受信装置の実施形態について示す模式図である。

【符号の説明】

101 擬似乱数列の出力装置

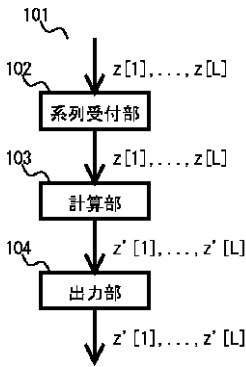
50 102 系列受付部



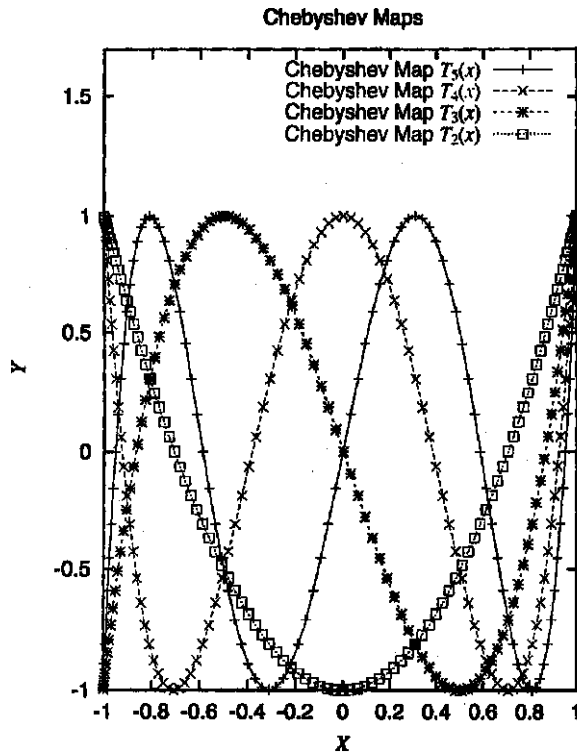
- 1 0 3 計算部
- 1 0 4 出力部
- 3 0 1 F I Rフィルタ
- 3 0 2 遅延回路
- 3 0 3 増幅器
- 3 0 4 加算器
- 3 0 5 端子
- 4 0 1 送信装置
- 4 0 2 信号受付部
- 4 0 3 系列出力部
- 4 0 4 拡散部

- 4 0 5 信号送信部
- 5 0 1 伝送信号
- 5 0 2 擬似乱数列
- 5 0 3 出力信号
- 6 0 1 受信装置
- 6 0 2 信号受信部
- 6 0 4 系列出力部
- 6 0 5 逆拡散部
- 6 1 1 生成部
- 10 6 1 2 相関検波部

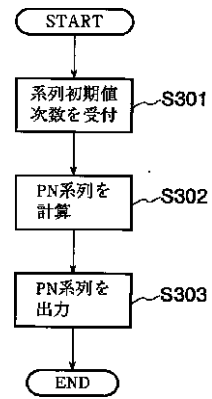
【図 1】



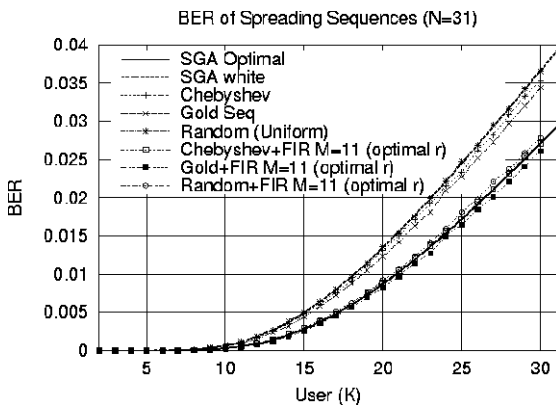
【図 2】



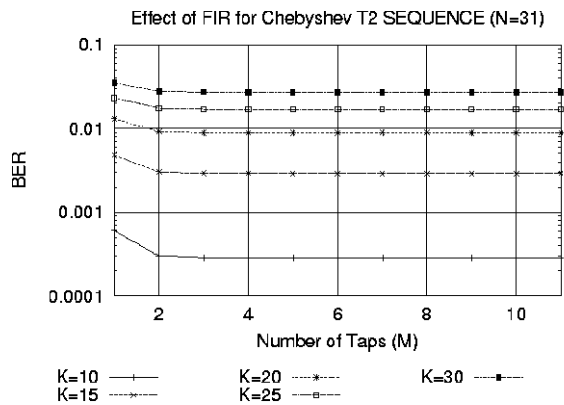
【図 16】



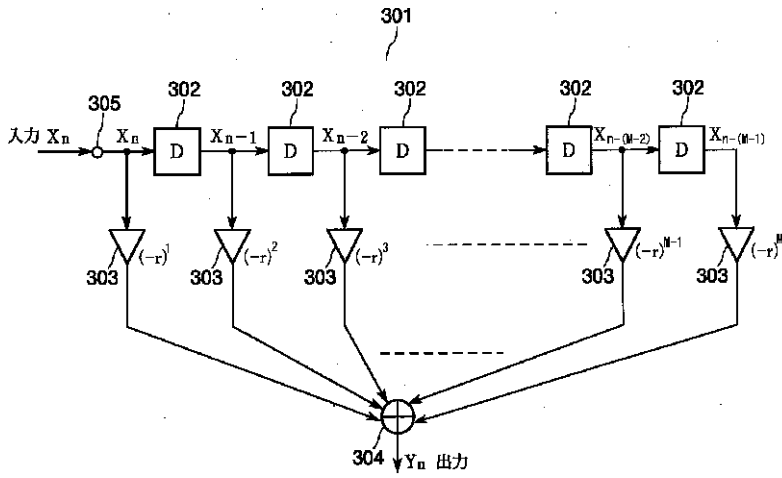
【図 4】



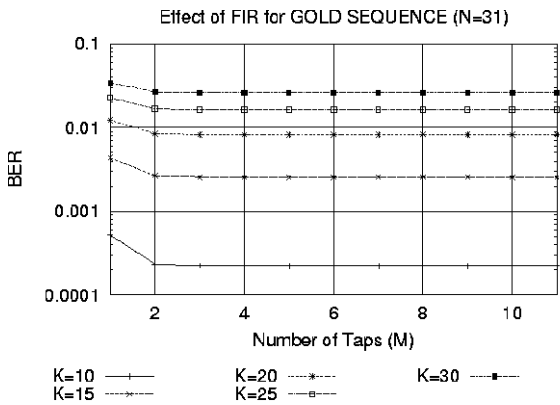
【図 5】



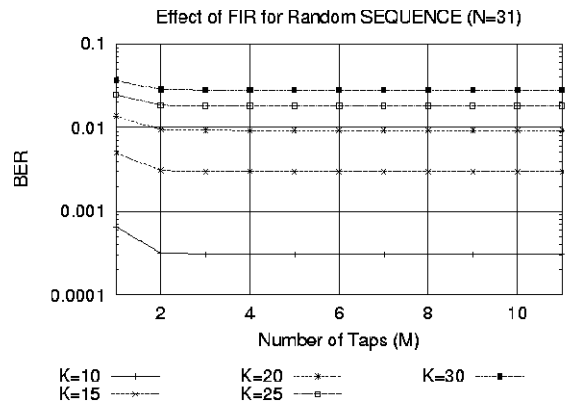
【 図 3 】



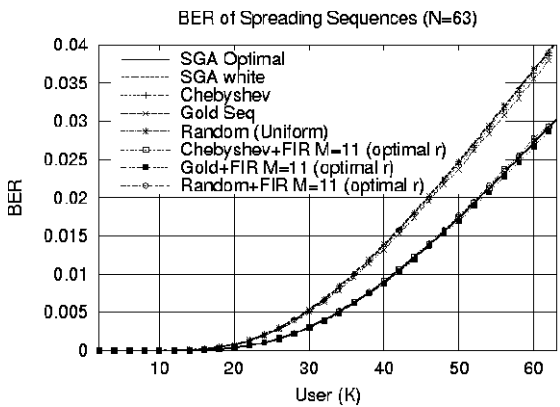
【 図 6 】



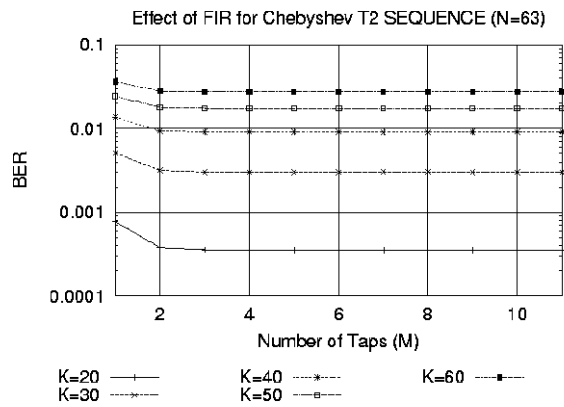
【 図 7 】



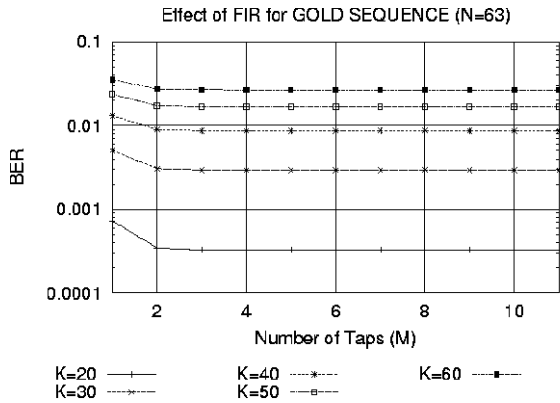
【 図 8 】



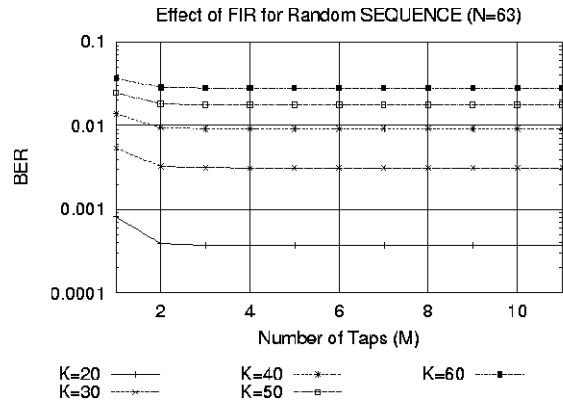
【 図 9 】



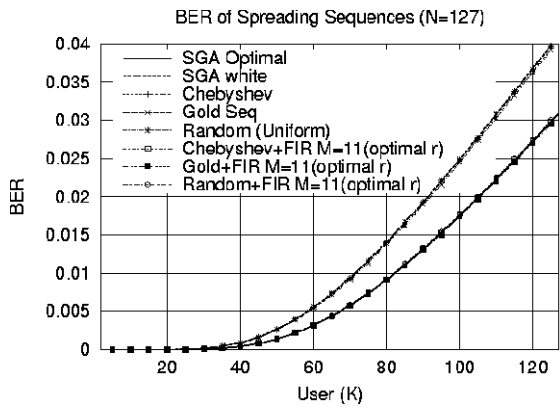
【 図 1 0 】



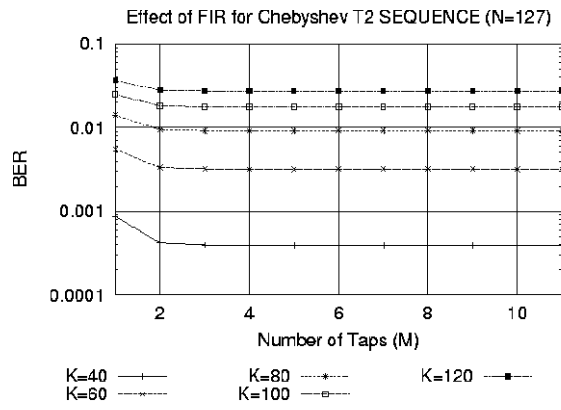
【 図 1 1 】



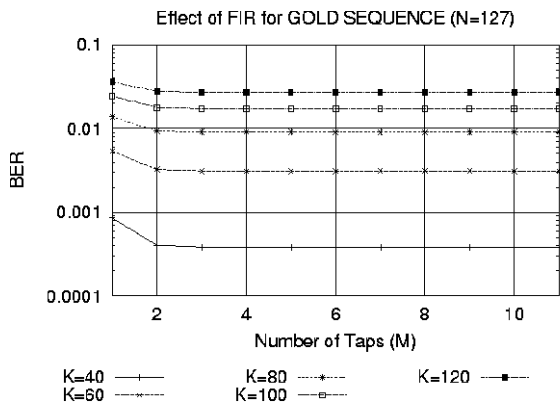
【 図 1 2 】



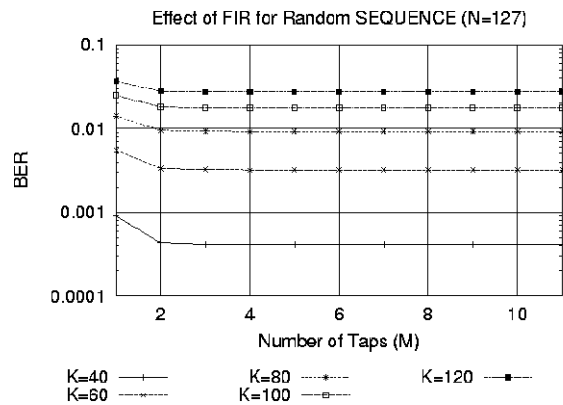
【 図 1 3 】



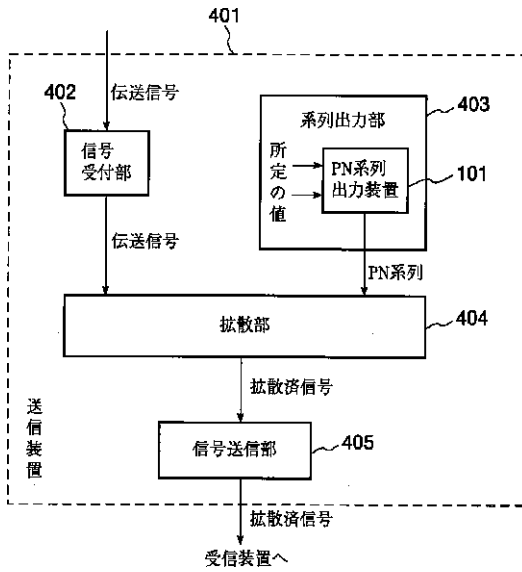
【 図 1 4 】



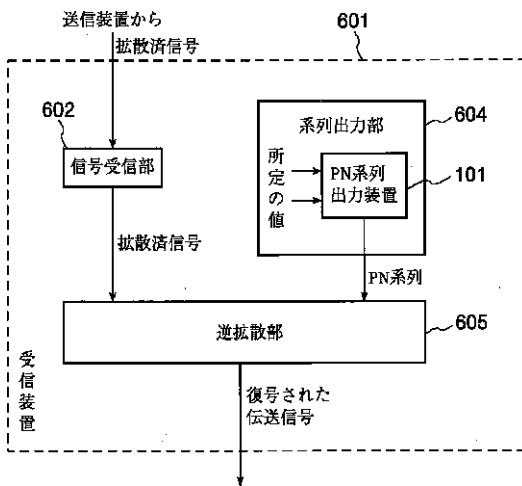
【 図 1 5 】



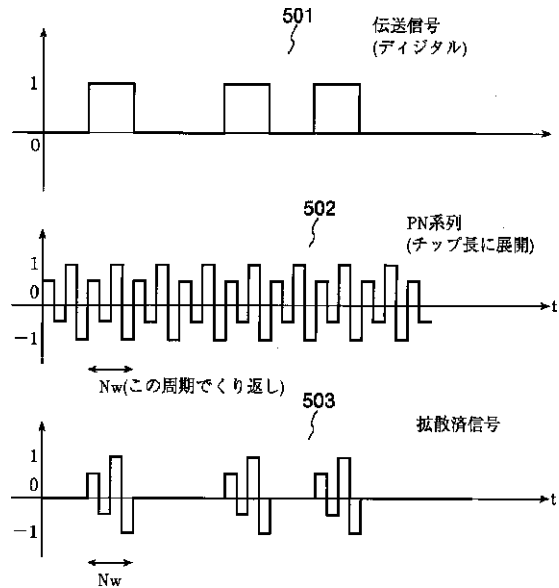
【図 17】



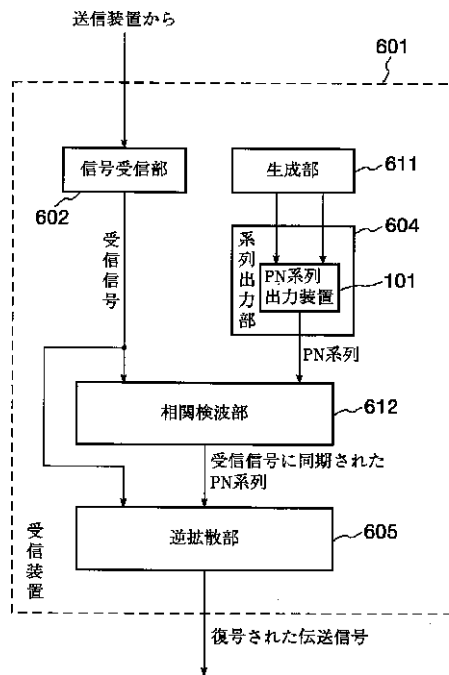
【図 19】



【図 18】



【図 20】



フロントページの続き

(71)出願人 501121439  
 山口 明宏  
 福岡県福岡市東区和白東 3 丁目30番 1 号  
 福岡工業大学 情報工学部 情報システム  
 工学科内

(72)発明者 梅野 健  
 東京都小金井市貫井北町 4 丁目 2 番地 1 号  
 総務省通信総合研究所内

(72)発明者 山口 明宏  
福岡県福岡市東区和白東 3 丁目30番 1 号  
福岡工業大学 情報工学部 情報システム  
工学科内

F ターム(参考) 5J104 FA08 NA04  
5K022 EE02 EE21 EE33